

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 March 2002 (21.03.2002)

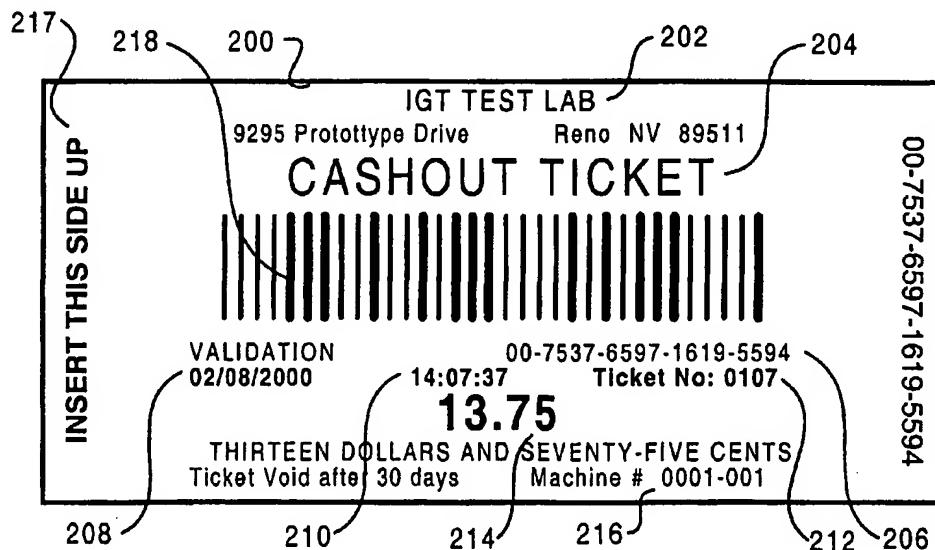
PCT

(10) International Publication Number
WO 02/22223 A2

- (51) International Patent Classification⁷: **A63F 13/00**
- (21) International Application Number: **PCT/US01/29112**
- (22) International Filing Date:
12 September 2001 (12.09.2001)
- (25) Filing Language: **English**
- (26) Publication Language: **English**
- (30) Priority Data:
09/660,984 13 September 2000 (13.09.2000) **US**
- (71) Applicant: **INTERNATIONAL GAME TECHNOLOGY [US/US];** 9295 Prototype Drive, P.O. Box 10580, Reno, NV 89511 (US).
- (72) Inventors: **PRASAD, Bhavani;** 9738 Thunder Mountain Way, Reno, NV 89511 (US). **ESPIN, Marc;** 5226 Canyon Run Drive, Sparks, NV 89436 (US). **ROWE, Richard, E.;** 4685 Spring Drive, Reno, NV 89502 (US).
- (74) Agent: **WEAVER, Jeffrey, K.;** Beyer Weaver & Thomas, LLP, 2030 Addison Street, P.O. Box 778, 7th Floor, Berkeley, CA 94704 (US).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: TRANSACTION SIGNATURE



(57) Abstract: The present invention provides systems and methods for protecting transaction information stored in a database of a gaming network. To accomplish this, a transaction signature is generated each time the user completes a transaction on a gaming machine. The transaction signature is generated using transaction information from a particular transaction. The transaction signature and transaction information are stored together in a network database. Upon subsequent access to the transaction information in the database, the transaction signature for the transaction information is recalculated based on the transaction information at that time. The new transaction signature is then compared to the transaction signature previously stored. Any differences between the two transaction signatures may be used to signal unauthorized alteration in the database transaction information.

WO 02/22223 A2



Published:

— without international search report and to be republished
upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TRANSACTION SIGNATUREBACKGROUND OF THE INVENTION

This invention relates to information security for gaming machine networks.

5 More particularly, the present invention relates to protecting gaming machine transaction information stored in a database from unauthorized alteration.

Gaming machines are becoming increasingly sophisticated. Many slot machines now employ CRT video display screens in place of more traditional mechanically-driven reel displays. Further, poker and other games of chance are now commonly provided on
10 electronic/video machines.

To control and monitor gaming machine activity, many establishments employ networks electronically linking numerous gaming machines. Frequently casinos connect their gaming machines to a local area network. Some casinos have even connected multiple local area networks to wide area networks spanning multiple casinos. Such
15 wide area networks allow groups of slot machines at various casinos to be connected to one another for various purposes including use in "progressive" games. Progressive games allow jackpots from multiple machines in multiple locations to grow as one large jackpot.

Transaction currency on gaming machines is also becoming more sophisticated.
20 Where once only coin handling mechanisms were present on gaming machines, credit devices such as cash-out vouchers now find wide use. These credit devices electronically store user transactions and, when used in conjunction with electronic processing systems, they monitor user activity. Some casinos now issue magnetic player identification cards that players use to obtain awards for frequent playing. A player
25 holding such card inserts it in a card reader provided on a gaming machine before he or she begins play. Accounting software on the local area network then detects the card insertion, notes the player identity and follows the machine activity. Other casinos now issue bar-coded tickets. When a player terminates interaction on a gaming machine, the gaming machine prints out a ticket, which includes the player's final status such as the
30 time and a cash-out value. The player then retrieves the ticket and may redeem it for credit at another game or cash it out at a change booth or a pay machine.

As mentioned, gaming transactions are now electronically stored, typically by the gaming machine network. Thus, each time a user completes a transaction on a gaming machine, the network stores the transaction information such as the time, the machine number and credit value of the device at transaction completion. When the user attempts
5 to play another game with the credit device, the network must redeem the value of the device, e.g., for game credit. Similarly, when the user attempts redeem the device for a cash-out, the network must provide the cash value of the device. Upon redemption of the device at a gaming machine or at cash-out, the redemption value of the device is determined according to the user's last stored transaction in the network.

10 Transaction information for the network is typically stored in a common location or database for consistent access by the gaming machines and casino personnel. Some casinos use conventional database management tools to store the transaction information. These database management tools generally permit open access for individuals on the network, e.g., casino personnel. Unfortunately, this open access to the database also
15 potentially allows authorized, and even in some cases unauthorized, individuals to tamper with the transaction information. In one example, an unscrupulous person could alter the transaction amount in a database record from \$10 to \$100.

From the foregoing, it should be apparent there exists a need for security measures that prevent tampering of transaction information stored in a database of a
20 gaming network.

SUMMARY OF THE INVENTION

The present invention provides systems and methods for protecting transaction information stored in a database of a gaming network. To accomplish this, a transaction
25 signature is generated each time the user completes a transaction on a gaming machine. The transaction signature is generated using transaction information from a particular transaction. The transaction signature and transaction information are stored together in a network database. Upon subsequent access to the transaction information in the database, the transaction signature for the transaction information is recalculated based
30 on the transaction information at that time. The new transaction signature is then compared to the transaction signature previously stored. Any differences between the

two transaction signatures may be used to signal unauthorized alteration in the database transaction information.

Generating the transaction signature from the transaction information may be performed by various methods. Typically, this occurs each time the user completes a transaction with a gaming machine. In some embodiments, certain transaction attributes or elements of those attributes are encrypted to generate the transaction signature. The encryption may change over time in order to increase security of the transaction information in the database.

In other embodiments, a portable credit device such as a ticket or card is carried by the player and used during interaction with the gaming machines. Each time the user finishes interaction with a particular gaming machine, the credit device is provided to the player with some of the updated transaction information. The credit device may have a magnetic strip or a semiconductor memory, for example, to store this information. For a ticket, the transaction information may be divided into elements such as a ticket validation number, a ticket amount, a ticket print time and date, a machine identifier, a cluster controller address and a ticket status. One or more of these transaction information elements may be used to generate the transaction signature. The transaction information and transaction signature are stored together in the database.

At a subsequent time, when the transaction information is to be updated or called from the database, the transaction information and transaction signature are verified. This may occur, for example, when the player presents the credit device for redemption at another machine or at cash-out station. At that time, the transaction signature is recalculated based on the current transaction information from the device. This recalculated transaction signature is compared with the stored transaction signature in the database. If the two transaction signatures are consistent, the transaction information may be updated or accessed. At this point, the credit can be redeemed. If the two transaction signatures are inconsistent, the transaction information update or request may be stopped and further investigation may ensue. In addition to verifying the transaction signature, the transaction information may also be compared between the transaction information in the database and transaction information currently available from the device.

These and other features and advantages of the invention will be described in more detail below with reference to the associated figures.

BRIEF DESCRIPTION OF THE DRAWINGS

5 FIG. 1 is a schematic diagram of a gaming machine network allowing electronic transfer of transaction information between a central database and casino gaming machines in accordance with the present invention.

 FIG. 2A illustrates an exemplary bar-coded ticket in accordance with one embodiment of the present invention.

10 FIG. 2B illustrates an exemplary portion of code containing the transaction information and a transaction signature in accordance with a specific embodiment of the present invention.

 FIG. 3 illustrates a process flow to generate a transaction signature in accordance with one embodiment of the present invention.

15 FIG. 4 illustrates a process flow to verify a transaction signature in accordance with one embodiment of the present invention.

 FIG. 5 illustrates an exemplary database for storing transaction information with transaction signature's in accordance with a specific embodiment of the present invention.

20

DESCRIPTION OF THE PREFERRED EMBODIMENTS

 The present invention will now be described in detail with reference to a few preferred embodiments thereof as illustrated in the accompanying drawings. In the following description, numerous specific details are set forth in order to provide a
25 thorough understanding of the present invention. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without some or all of these

specific details. In other instances, well known process steps and/or structures have not been described in detail in order to not unnecessarily obscure the present invention.

According to the present invention, transaction information stored in a database or other data repository is secured by recording a transaction signature each time the
5 player completes a transaction with a gaming machine. The transaction signature is computed using certain elements of the gaming transaction information. The transaction information and transaction signature are stored together and verified each time the transaction information is accessed. Any inconsistency in the transaction information or transaction signature between the current values and those previously stored may be used
10 to identify a transaction information discrepancy. This ensures that a person, such as someone gaining unauthorized access to the transaction data or even a privileged user, cannot alter the stored transaction information. Thus, it becomes much more difficult to cheat a casino by increasing the amount of credit associated with a transaction.

FIG. 1 is a schematic diagram of a gaming machine network 100 that may be
15 used with the present invention. The network 100 includes a number of gaming machines 102. The gaming machines 102 permit a player to enter coins, bills, tickets or any other form of credit to begin a transaction between the player and a gaming machine. Upon completion of a transaction with a gaming machine 102, the player is issued a portable credit device, which will be described below. The gaming machine itself may
20 issue the credit device. The network 100 electronically transfers transaction information between a central database 101 and the gaming machines 102. For this purpose, the network 100 includes lines or cables 104, which may take various forms including coaxial wires, wireless connections or fiber optic cable.

In some embodiments, numerous machines 102 connect to a single cluster
25 controller or a Clerk Validation Terminal (CVT) 106. In one embodiment, a single CVT 106 may accommodate up to 64 machines. The CVT 106 may store transaction information associated with the gaming machines 102. More specifically, the CVT 106 may store credit device information corresponding to the outstanding devices that are waiting for redemption. Any of the machines connected to the CVT 106 will accept
30 credit devices from other gaming machines connected to the same CVT 106. The CVT 106 may also contain additional memory for retaining redundant credit device

information. This may be used as a secondary storage medium for credit device information recovery in the event of power failure or memory loss to the main memory in the network 100. In addition, players may redeem credit devices for cash at the CVT 106 at any time.

5 As there may be many groups of gaming machines 102 in a large casino or other establishment, multiple CVTs 106 may be implemented. The CVTs 106 are connected to a local area network (LAN) 107 which includes a number of computers or workstations as well as terminals, disk drives with fixed and/or removable media, printers and other peripherals connected on a token ring network. The computers on the
10 LAN 107 may provide the casino with various functions such as processing jackpots and fills, exporting of transaction information to the central accounting system, and generating accounting reports and security reports, etc. Other components connected to LAN 107 may include multiplexers, modems, and phone lines to an external system.

 The LAN 107 also includes information services components 108. Information
15 services 108 includes a central database 101 and a front end controller 109 which acts as a general controller for the network 100. The controller 109 may continuously poll the various CVTs 106 requesting information pertaining to gaming transactions in the network 100. The CVTs 106 are, in turn, continuously polling the various machines 102. For example, if a credit device has been inserted in a gaming machine 102, that
20 machine will communicate an insertion event to its CVT 106 in response to the next CVT 106 poll. Then when the front end controller 109 polls the CVT 106, the CVT 106 communicates the insertion event to the front end controller 109.

 The LAN 107 includes numerous work stations. A cashier's station 112 is included for redemption of credit devices created within the network 100. The cashier's
25 station 112 includes a computer 114 with a printer 118 and a bar-code scanner 116 for reading credit devices. The network 100 may accommodate as many cashier stations 112 as required to support a facility.

 Additional stations may be included in the LAN 107. For example, the LAN 107 and may include a station in charge of security and a workstation in charge of
30 surveillance. A soft count station 120 may also be included for daily verification of bills and tickets accepted gaming machines 102 in the network 100. An audit station 122 may

also be included for accounting purposes. Any of the stations in the LAN 107 may provide the current status of a credit device. Each of the stations on the LAN 107, including the front end controller 109, may be implemented on any of a variety of commercially available computer systems. Such machines include, but are not limited to, PC compatibles, DEC VAXs, and UNIX machines. In alternative embodiments, the various network functions such as front end control are accomplished by distributed processing. In such cases, the network functions are performed on multiple nodes.

In the depicted example, information services 108 also includes a file server 124 which is the main processor in the network. Its functions will be described in more detail below. A suitable file server machine is the Compaq 550 available from Compaq Computers. The file server communicates with all stations included on the LAN 107 in addition to an external host network through a modem.

As is known to those of skill in the art, EFT hosts are typically mainframe computers which route electronic funds transfer requests and authorizations between various sales or services establishments (a casino in this instance), and remote funds repositories such banks or credit unions. Compaq Computers provides many of the file server computers now used for this purpose. And ACI Company of Omaha, NE provides much of the banking software or "switch processing" software used by most of the major networks around the world. The EFT system may also include workstations, printers, multiplexers, modems, etc. connected as a network and communicating with the casino to the individual card issuing institutions over phone lines.

EFT hosting may be provided by various widely used EFT service providers such as Cirrus™ and Interlink™. Such EFT service providers contract with various card issuing institutions (e.g., banks or other financial institutions) to provide EFT services. In some instances they also contract with one or more very large EFT service providers such as Maestro™ and Interlink™ which together provide EFT services for most of the available funds repositories. Such services are further described in commonly owned United States Patent Application entitled "Cashless Transaction ClearingHouse" filed August 25, 2000, which is incorporated by reference herein for all purposes.

In some embodiments, the EFT host will be provided and maintained by a casino or gaming machine vendor. All EFT requests from gaming machines of the vendor or

casino would, in such cases, be routed through the private EFT host. In addition, the host could process ATM, check authorization, and point of sale transactions within the casino. In such embodiments, the casino or gaming machine vendor providing hosting preferably contracts with the large service providers (e.g., Maestro™ and Interlink™),
5 rather than contracting with the smaller providers or the individual funds repositories.

When a user wishes to play a gaming machine 102, he or she inserts credit through a credit acceptor included in the machine. The credit may include cash, coins, game tokens or credit devices such as tickets and magnetic cards. The credit acceptor may be a coin acceptor, bill validator or a similar device which reads tickets or other
10 suitable credit devices. The cash, game tokens or tickets may be stored in the interior of the gaming machine in devices including ticket stackers, drop boxes, and token dispensers. At the start of interaction with the gaming machine, the player may enter player tracking information using a card reader, a keypad, and a florescent display. During the interaction, the player views game information using a video display.
15 Usually, during the course of a game, a player is required to make a number of decisions that affect the outcome of the game. The player makes these choices using a set of player-input switches.

After the player has completed interaction with the gaming machine, the player may receive a portable credit device from the machine which includes any credit
20 resulting from interaction with the gaming machine. By way of example, the portable credit device may be a ticket having a dollar value produced by a printer within the gaming machine. A record of the credit value of the device will be stored in a memory device provided on the network 100 (e.g., a memory device associated with CVT 106 and/or database 101). Any credit on the device may be used for further games on other
25 gaming machines 102. Alternatively, the player may redeem the device at a designated change booth or pay machine.

Having briefly discussed an exemplary gaming system suitable for use with of the present invention, the transaction information protection aspects of the invention, as well as other features and advantages of the present invention, may be better understood with
30 reference to the figures and discussions that follow. As mentioned earlier, the present

invention implements a transaction signature to provide transaction information protection.

In a preferred embodiment of the present invention, a portable credit device is carried by the player. The credit device may be a magnetic card, cash voucher, ticket, or
5 any other form of portable credit device. Fig. 2A illustrates a ticket 200 in accordance with a specific embodiment of the present invention.

The ticket 200 displays one or more transaction information elements. The transaction information elements may include, for example, a casino identification 202, a ticket identification 204, a validation number 206, a date 208, a time 210, a ticket
10 number 212, a value 214, and a machine identification number 216. The validation number 206 is a unique number generated within the network 100 such that each ticket 200 and transaction may be uniquely identified. In one embodiment, the time 210 refers to the time when the ticket 200 is printed. Other transaction information elements not shown which may be stored on the tickets 200 include a cluster controller address, ticket
15 status, status change time and other related information. The ticket 200 may also display other information to assist the player such as instructions 217. The ticket 200 is typically produced each time a player completes a transaction on a gaming machine.

The ticket 200 also includes a bar-code 218. The bar-code 218 stores one or more of the transaction information elements and transaction data in a manner which is
20 readable by gaming machines 102 in the network 100. The bar-code 218 may include any of the transaction information elements listed above. For example, the bar-code 218 may include the validation number 208 for unique identification of the ticket 200 by a gaming machine.

By way of example, the ticket 200 may be a ticket used in the EZPay ticket
25 system. The EZPay ticket system is fully described in commonly owned U.S. Patent Application No. 09/544,884 entitled "Wireless Gaming Environment", which is incorporated herein by reference. Although the present invention is primarily discussed with respect to the ticket 200, which the user carries, any suitable portable or transferable credit device capable is suitable for use with the present invention.

As mentioned earlier, the present invention generates a transaction signature to protect transaction information from tampering. The transaction signature is computed using one or more of the transaction information elements (e.g., a combination of casino ID, time, and value). Generating the transaction signature may be performed at various
5 times and from various sources. In a preferred embodiment, a transaction signature is generated by a main processor in conjunction with the network central database each time the user completes a transaction with a gaming machine. In this case, the transaction signature is generated from transaction information elements included in the most recent transaction. The transaction signature may also be generated from other
10 information such as the status of the credit device, the time the ticket was generated, the amount on the ticket, etc. After generation of the transaction signature, the transaction information and transaction signature are stored (preferably in the central database) for subsequent access and verification.

Generally speaking, a transaction refers to interaction of a player with a gaming
15 machine. Typically, the transaction begins when the player inserts credit into the machine. The transaction includes the player participating in one or more games on the machine. Usually, during the course of a game, the player is required to make a number of decisions that affect the outcome of the game. After the player has completed interaction with the gaming machine, the transaction is finished and the player may
20 receive a credit device from the machine which includes any credit resulting from interaction with the gaming machine.

The transaction information used for generating the signature may vary. Broadly speaking, the transaction information used in generating the transaction signature may include any data or information related to a transaction between a player and a gaming
25 machine. The transaction information used for generating the transaction signature need not be characteristic or unique by itself, but may be processed to provide a characteristic transaction signature. A characteristic transaction signature refers to a transaction signature which is substantially unique within a database. In some embodiments, the transaction information used for generating the signature may include the user's
30 identification (e.g., name or number), transaction termination time, a machine identifier, casino identification, final transaction value, ticket validation number, ticket printer time, machine identifier, cluster controller address, ticket status, or some combination thereof.

Any technique for generating the transaction signature from the chosen transaction information (the seed value(s)) may be employed. Preferably, it is a technique that cannot be readily discerned from the other information stored with the signature (e.g., other information in a database record). In some embodiments, a specific
5 algorithm is used to translate the transaction information into the transaction signature. The resulting transaction signature produced by the algorithm may take the form of a string of characters. The string of characters may include computer-generated symbols such as numbers, letters, symbols, etc. For simplicity, the transaction signature is preferably provided "in the clear"; i.e., without encryption of the string of characters. In
10 another embodiment, the string of characters may be encrypted to improve protection. As one skilled in the art would appreciate, there exists an abundant number of ways to create an encrypted key from the transaction information and the present invention may include any such encryption algorithm or mechanism.

In other embodiments, the algorithm used to produce the transaction signature
15 may vary over time to improve transaction information protection. By way of example, the algorithm may change every week. In one embodiment, the information used in generating the signature may change. For example, in one week, the transaction information used for generating the signature of a ticket may include the user's name, the ticket print time and a machine identifier. The next week, the transaction information
20 used for generating the signature may include the user's name, the gaming machine identifier and the final transaction value on the gaming machine. In addition, the order of transaction information elements used to generate the transaction signature may also change to vary the algorithm and transaction signature.

One exemplary algorithm for creating transaction signatures suitable for use with
25 the present invention is a cyclic redundancy check (CRC) algorithm. To vary this CRC algorithm over time, the order of transaction information elements provided to the algorithm may vary as well as altering the initial seed value to the algorithm. Specific algorithms suitable for use with the present invention include the CRC-16 algorithm and the CRC-32 algorithm. As one skilled in the art would appreciate, there exists an
30 abundant number of algorithms to create an encrypted key from the transaction information and the present invention may include any such algorithm.

As mentioned, the transaction information and transaction signature are recorded electronically in a memory device within the network 100. FIG. 2B illustrates an exemplary data structure 250 containing the transaction data and a transaction signature in accordance with a specific embodiment of the present invention. The data structure 5 250 includes a header portion 252 used for transmission within the network 100. A transaction information portion 254 contains some or all of the transaction information. This may include the transaction time, validation number, ticket amount, etc. A transaction signature portion 256 contains the transaction signature corresponding to the transaction information contained in the transaction information portion 254. In one 10 embodiment, the data structure 250 is included in a network packet sent over a network from a central database to a gaming machine. This may occur, for example, when the gaming machine requests validation of a ticket from the central database.

FIG. 3 illustrates a process flow 300 to record a transaction signature after a player completes one or more games on a playing machine in accordance with one 15 embodiment of the present invention. Processes in accordance with the present invention may include up to several additional steps not described or illustrated here in order not to obscure the present invention.

The process flow 300 begins with a request to finish interaction with a gaming machine (302). At this point, a processor within the machine may calculate one or more 20 transaction elements associated with the transaction, e.g., the time and cash out value. The cash out value after interaction with the gaming machine may include winnings from the gaming machine. The transaction elements are then sent to a central processor for the network which is coupled to a central database. The central processor then identifies one or more transaction information elements associated with the cash out transaction 25 (304). These elements are then used to calculate a transaction signature for the transaction (306).

The transaction information and transaction signature may then be stored (308). In one embodiment, the transaction information and transaction signature are recorded in the central database of the gaming network. In addition, the transaction information and 30 transaction signature may also be recorded in additional memory locations such as those found in a cluster controller or CVT, for example. The transaction information and

transaction signature may be stored in various ways. In one embodiment, the transaction information and transaction signature are stored together as a new record in a database after each transaction. In another embodiment where transaction information is updated in a progressive record, each time transaction information is updated in the database, an
5 updated transaction signature is automatically attached to the transaction information. In this manner, the most recent transaction signature is verified whenever the transaction information is accessed.

Upon subsequent access to the transaction information, either for redemption by a gaming machine or at cash-out, the transaction signature is verified. Verifying the
10 transaction signature includes verification between the transaction signature stored in the database and a transaction signature calculated based on the transaction information at the time of access. The transaction information used at the time of access may include transaction information obtained from a credit device used with a gaming machine. Any discrepancies between the current calculated transaction signature the transaction
15 signature stored in the database may be investigated. In this manner, any alteration to the transaction information in the database may be detected. In some embodiments, the transaction information may additionally be verified upon subsequent access to the transaction information. Verifying the transaction information may include verification between the transaction information stored in the database and the transaction
20 information at the time of access by a credit device in a gaming machine, for example.

In one embodiment, a transaction signature is verified each time transaction information related to the transaction signature is updated and each time the transaction information is accessed, e.g., for redemption at a cashier's station. Note that this need not be associated with a credit transaction such as redemption. It may also occur at
25 random times, when triggered by a database integrity check, for example. In one embodiment, when credit devices are to be redeemed, only credit devices with valid transaction signatures are allowed redemption. In another embodiment, when transaction information is retrieved from the database to be sent to a CVT, a cashier's station or a gaming machine, only transaction information having a valid transaction signature is
30 sent. In either case, a system audit log may be created and maintained that contains the results of requests for transaction information and includes requests which contain requests for transaction information having invalid transaction signatures.

FIG. 4 illustrates a process flow 400 for validating a transaction signature in accordance with a specific embodiment of the present invention. Processes in accordance with the present invention may include up to several additional steps not described or illustrated here in order not to obscure the present invention.

5 As mentioned before, according to one embodiment, a player may carry a credit device for use with gaming machines of a gaming machine network. The player may redeem the credit device and any value on the credit device at any gaming machine, a designated cash out window or a pay machine. When a credit device is redeemed at a cash out window, the cashier may verify the device by inputting the device number into
10 the cashier station computer. In one embodiment where the credit device is a ticket including a bar-code, the cashier may input the ticket identification by scanning the ticket with a bar-code scanner. The most recent ticket transaction information and transaction signature will be stored in a central database of the system. Thus, upon receiving a request to validate a cash out transaction (402), the system will retrieve a record of the
15 transaction (404). The record of the transaction will include a transaction signature and any transaction information stored in the central database.

The process flow 400 then calculates the transaction signature from the relevant transaction information elements in the database record (406). The process flow 400 compares the calculated transaction signature with the transaction signature recorded in
20 the database (408). In addition, the process flow 400 may also compare one or more of the transaction information elements for consistency between the database and the credit device.

If the calculated transaction signature (from 406) matches the transaction signature recorded in the database (410), validation of the cash out transaction is allowed
25 (412). If the validation request occurs at a gaming machine, the player will be credited the corresponding amount on the gaming machine. If the validation request occurs at a cashier's station, the player will be paid with the corresponding amount according to the cash out value stored in the database. The system may also print out a verification receipt for each ticket at the cashier's station. The cashier may store the ticket and the
30 verification receipt. If the calculated transaction signature (from 406) does not match the

transaction signature recorded in the database (410), the cash out transaction is prevented (414), the discrepancy may be logged and investigated (416).

5 In one embodiment, the transaction signature and/or transaction information in the database are verified each time the validation number is accessed, each time the transaction information is updated, and each time credit associated with the validation number is to be redeemed. In some embodiments, the transaction information may be verified using a comparison between the stored transaction signature and a newly calculated transaction signature based on transaction information not in the database. In this case, the new transaction signature is generated using transaction information from
10 an alternate source outside the database at the time of access. By way of example, the alternate source may be the credit device used by the player. Again, if the two transaction signatures are different, the transaction information may have been altered and the discrepancy is logged and investigated.

15 In one embodiment, the network 100 may perform periodic validation of the transaction information in the database. In a specific embodiment, the network 100 performs periodic validation by comparing transaction signatures locally stored in the CVTs 106 with transaction signatures stored in the database. Any discrepancies between transaction signature stored in CVT's 106 and those in database may elicit further investigation.

20 The transaction information and transaction signature are stored within a database. The database may be centralized to the entire system or a database may included local to a CVT for a certain number of gaming machines. Any conventional database tool is suitable for use with the present invention. By way of example, a DBA or SQL database are both suitable for use with the present invention.

25 FIG. 5 presents a logical representation of a database 500 for storing transaction information with a transaction signature in accordance with a specific embodiment of this invention. The database 500 includes a number of records 501 each relating to an individual transaction. A primary key 502 uniquely identifies each record 501. In one embodiment, the primary key 502 is the validation number 206 produced by a gaming
30 machine at cash out of the credit device. Each record 501 may also include a number of transaction information elements such as a print time 504, a machine ID 506, a cashier

value validation and a redemption status 510. A transaction signature 512 is also included in each record 501. The database 500 may also include numerous other transaction information elements such as the machine number, the cluster controller number, or any other elements stored on the ticket 200.

5 In one embodiment, the transaction signature is generated and appended to the transaction information in the database whenever the transaction information is updated. In this manner, a transaction signature is attached to the transaction information in the database based on the most recent transaction information.

Advantageously, the present invention prevents unauthorized tampering of
10 transaction information stored in a database of a gaming network. Correspondingly, the transaction information stored in the database may be kept "in the clear". In other words, the transaction information may be kept in the database without encryption which may encumber transmission and thereby decrease performance of the network. The above-mentioned recording and verification of transaction signatures also prevents anyone with
15 a standard database tool to create new tickets in the system database and attempt to redeem such tickets at a cashier terminal, a cluster controller or machine in the network.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For instance, while the
20 methods and systems of this invention have been described primarily in reference to protecting the cash out value of the transaction information, the invention is not limited to protecting just this element of the transaction information. Indeed, the transaction information protected by the present invention may include any of the transaction information elements stored in the database such as the ticket identification, the time, the
25 validation number, etc. Therefore, the present examples are to be considered as illustrative and not restrictive, and the invention is not to be limited to the details given herein, but may be modified within the scope of the appended claims.

What is claimed is:

1. A method of protecting transaction information stored in a database associated with gaming machines, said method comprising:
 - 5 identifying a transaction resulting from player interaction with a gaming machine;
generating a first transaction signature from one or more transaction information elements included in the transaction;
recording the transaction information elements and the first transaction signature in the database; and
 - 10 verifying the first transaction signature.
2. The method of claim 1 wherein the player interaction with the gaming machine includes changing an amount of credit on a credit device used by the player to play the gaming machine.
- 15 3. The method of claim 2 wherein the first transaction signature is verified prior to a subsequent transaction.
4. The method of claim 1 wherein verifying the first transaction signature
20 comprises:
 - generating a second transaction signature from transaction information in the database; and
 - comparing the first transaction signature with the second transaction signature.
- 25 5. The method of claim 4 further comprising providing redemption of any credit on the credit device based on the verification.
6. The method of claim 5 wherein verifying occurs at a cashier station.
- 30 7. The method of claim 1 further comprising verifying the transaction information.

8. The method of claim 1 wherein the one or more transaction information elements include at least one of a ticket identification number, a ticket amount, a ticket print time, a machine identification, and a ticket status.
- 5 9. The method of claim 1 wherein generating the first transaction signature comprises calculating the first transaction signature from the one or more transaction information elements using a first algorithm.
- 10 10. The method of claim 9 further comprising generating a second transaction signature from the one or more transaction information elements using a second algorithm, the second algorithm being different from the first algorithm and being used at a different time than the first algorithm.
11. The method of claim 1 wherein the first transaction signature is characteristic.
- 15 12. The method of claim 1 wherein verifying the first transaction signature is performed by a central processor.
13. The method of claim 1 further comprising cashing out credit associated with the transaction after verifying the transaction signature.
- 20 14. A method of using a credit device on a gaming machine in a gaming machine network, the method comprising:
- 25 initiating interaction between the gaming machine and a player;
terminating interaction with the player;
recording a set of transaction information elements related to the interaction;
generating a transaction signature from one or more of the set of transaction information elements;
- 30 recording the transaction signature with the set of transaction information elements; and
providing the credit device to the player.

15. The method of claim 14 wherein initiating the interaction uses one of a coin, a game token, or the credit device.
16. The method of claim 14 wherein the set of transaction information elements
5 include at least one of a date, a transaction number and a credit device value.
17. The method of claim 14 wherein the transaction information and the transaction signature are stored within a database of the gaming machine network.
- 10 18. The method of claim 14 wherein the credit device is a ticket.
19. The method of claim 14 further including initiating interaction with a second gaming machine in the gaming machine network using the credit device.
- 15 20. The method of claim 19 the further including verifying the transaction signature before initiating interaction with the second gaming machine.
21. A database for use in a gaming machine network, the database comprising a set of records, each record comprising a first portion including a primary key which
20 uniquely identifies the record within the set of records, a second portion including one or more transaction information elements, and a third portion including a transaction signature.
22. The database of claim 21 wherein the transaction information elements include at
25 least one of a ticket identification number, a ticket amount, a ticket print time, a machine identification and a ticket status.
23. The database of claim 21 wherein the transaction signature is produced from one or more of the transaction information elements using an algorithm.
- 30 24. The database of claim 21 wherein one of the one or more transaction information elements may not be updated unless the transaction signature is verified.

25. A cashless instrument transaction network for validating the use of cashless instruments across separate gaming properties, each of which generates and validates cashless instruments, the cashless instrument transaction network comprising:

- 5 a network interface allowing the cashless instrument transaction network to communicate with each of the separate gaming properties; and
- a processor configured or designed to (i) receive cashless instrument validation requests via the network interface from a first property for a cashless instrument presented at the first property (ii) verify a transaction signature generated from one or
- 10 more transaction information elements included when the instrument was generated previously with one or more transaction information elements included in the cashless instrument presented at the first property.

- 15 26. The cashless instrument transaction network of claim 25, wherein the transaction signature was generated previously from a second property.

27. The cashless instrument transaction network of claim 25, wherein the first property is one of a gaming machine and a cashier's station.

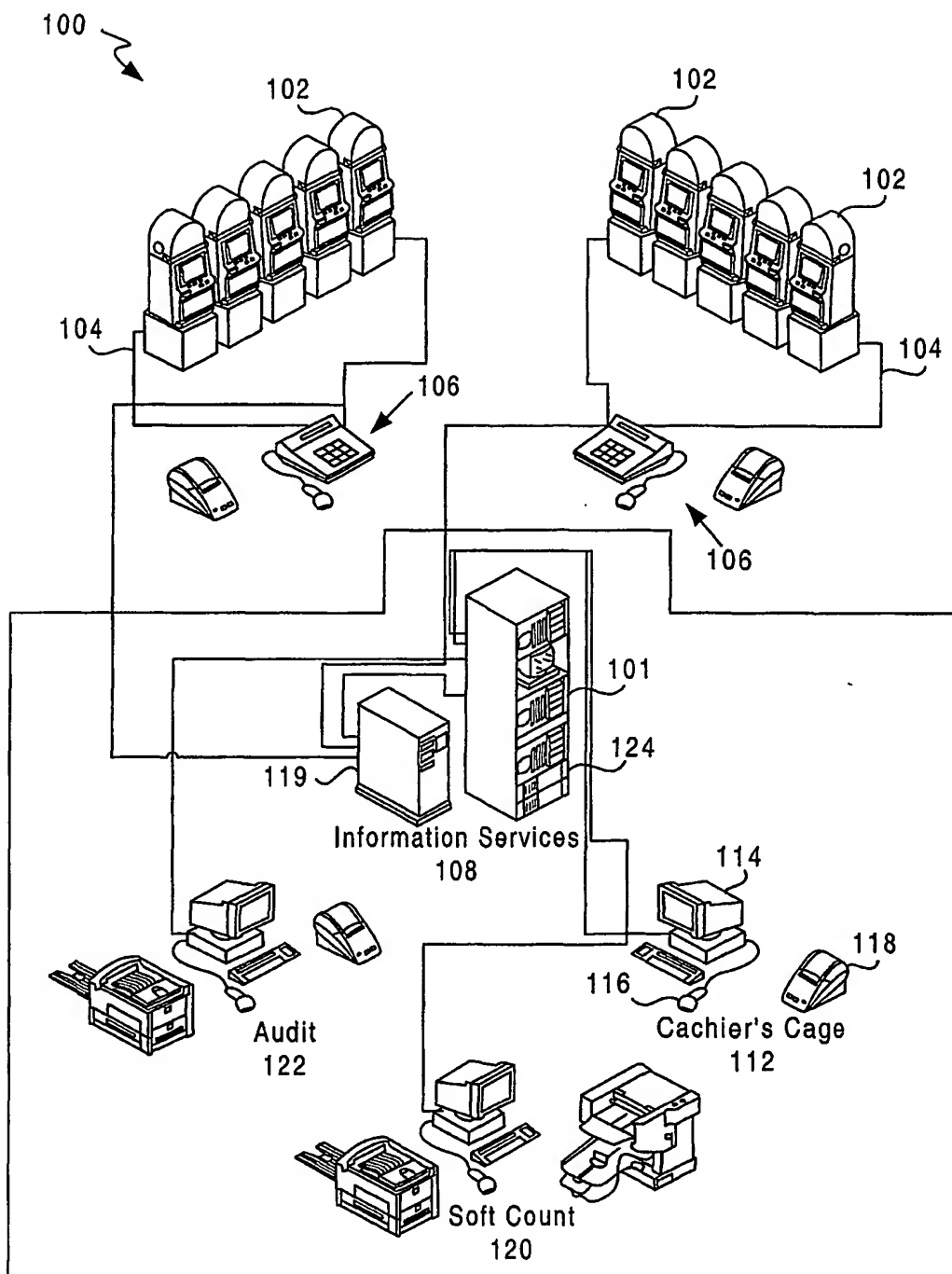
20

28. The cashless instrument transaction network of claim 25, further comprising a transaction database containing cashless instrument transaction information.

29. The cashless instrument transaction network of claim 28, wherein the database
- 25 further comprises transaction signatures associated with the cashless instrument transaction information.

30. The cashless instrument transaction network of claim 25, wherein the cashless instrument is selected from the group consisting of a smart card, a debit card, a bar-
- 30 coded ticket and an EZ pay ticket voucher.

1/5

**FIG. 1**

2/5

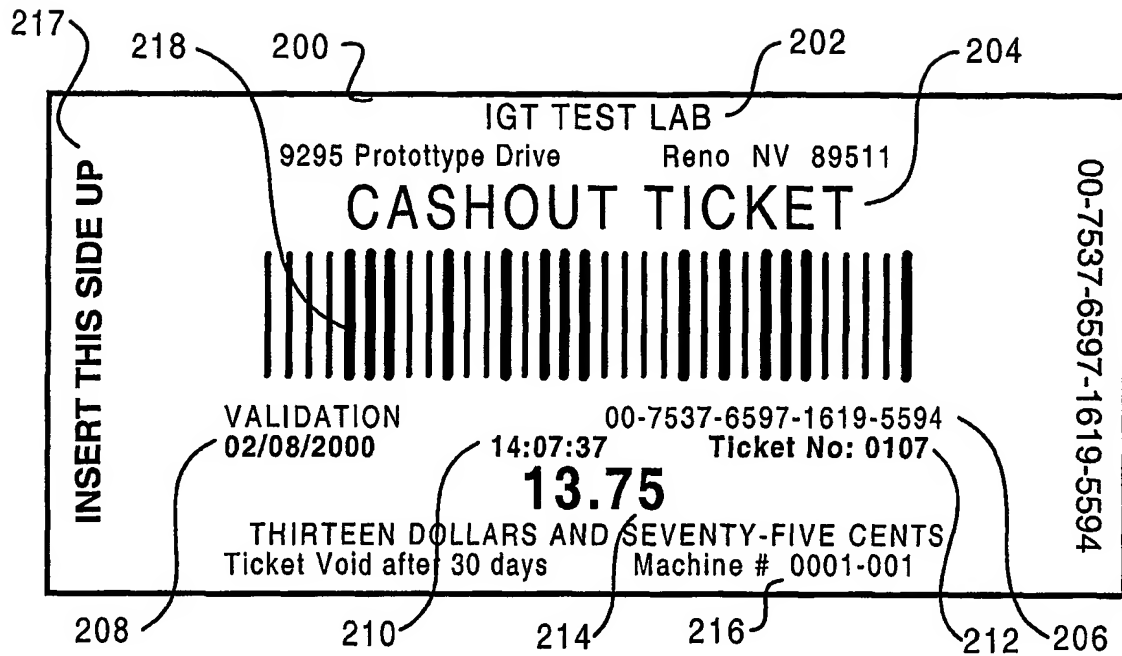


FIG. 2A

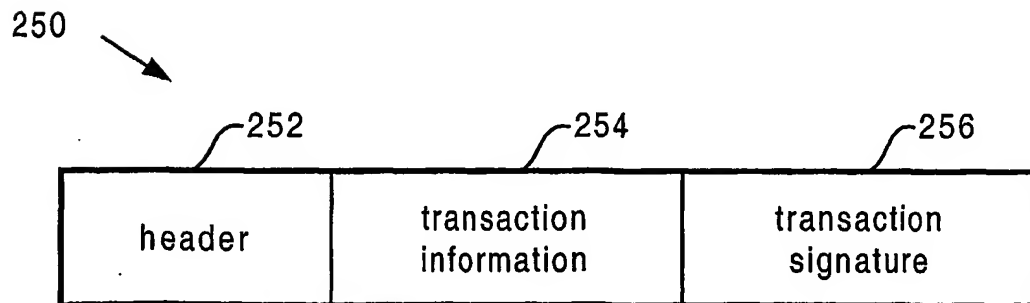


FIG. 2B

3/5

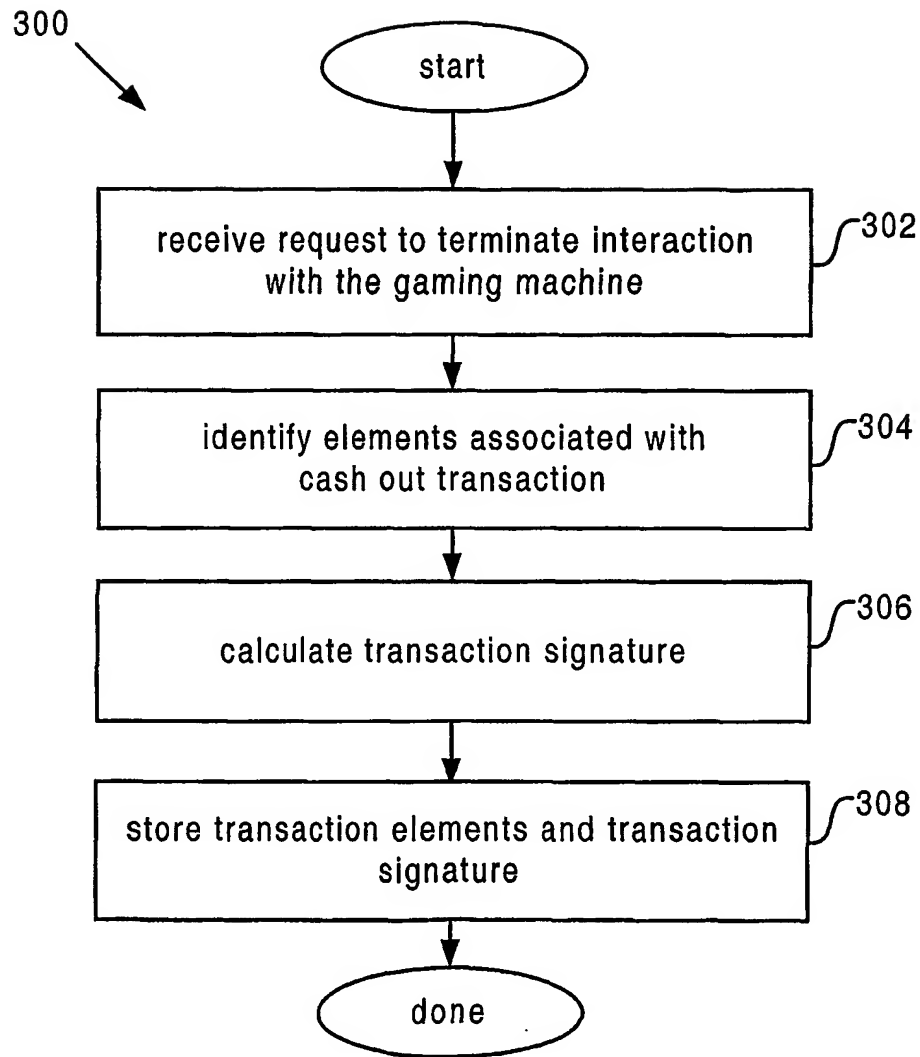


FIG. 3

4/5

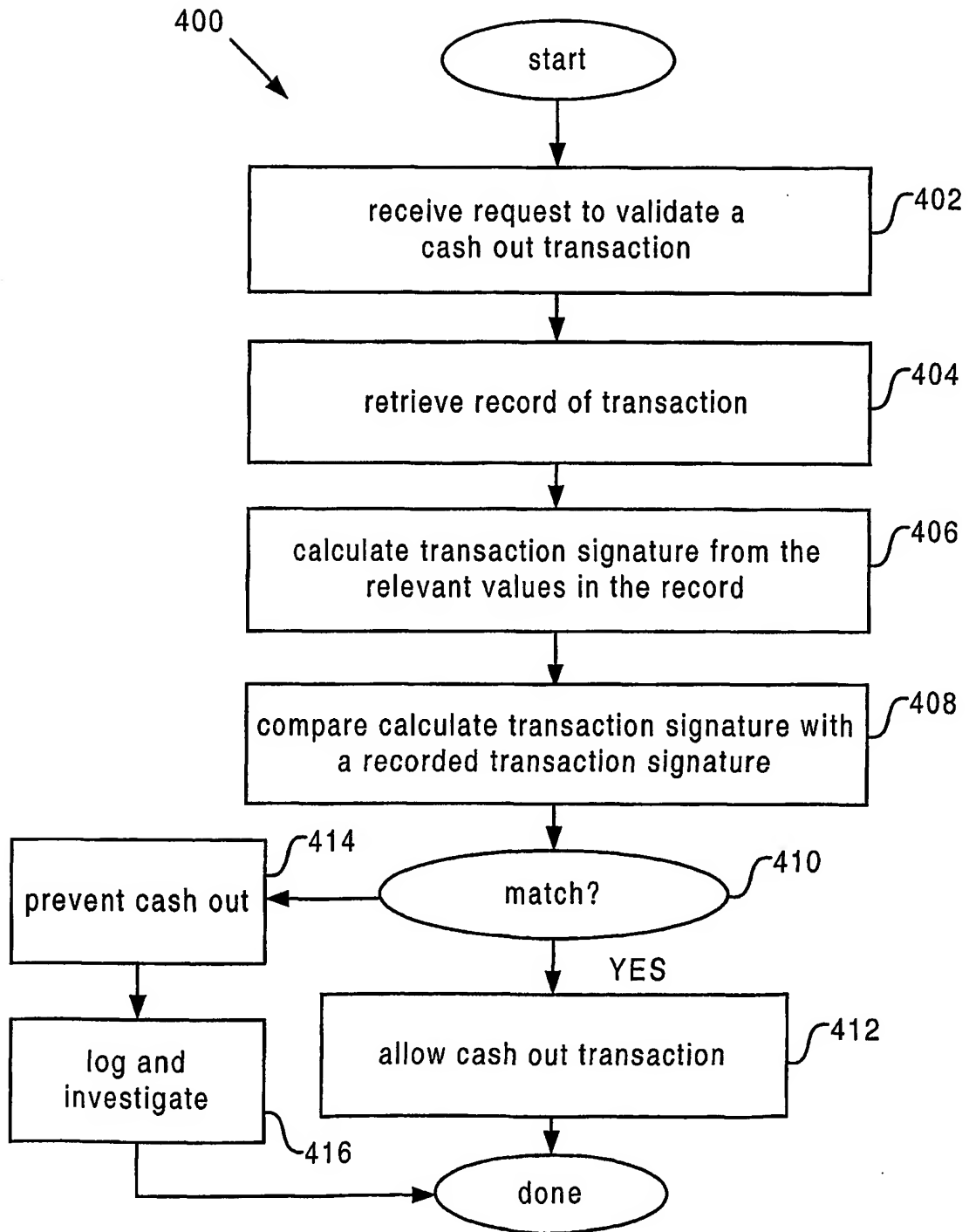


FIG. 4

5/5

500

| 502 | 504 | 506 | 508 | 510 | 512 |
|---------------------------------------|----------------------|-----------------|-------------------|----------------------|--------------------------|
| Validation Number (Primary Key) | Print Time | Machine I.D. | Cash-Out Value | Redemption Status | Transaction Signature |
| 000001 | 02/08/00 15:32:58 | 0392 | \$10.00 | unpaid | x9l03a*o |
| 000002 | 02/12/00 15:33:21 | 0028 | \$2.25 | unpaid | p29%gu*sd |
| 000003 | 02/12/00 15:33:25 | 1021 | \$1000.00 | paid | iu5%lk09D |
| 000004 | 02/12/00 15:38:43 | 0552 | \$30.00 | unpaid | jj!7yh#k\$ |
| 000005 | 02/12/00 15:39:03 | 0983 | \$5.75 | paid | zre(*2<kl |

501



FIG. 5

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 March 2002 (21.03.2002)

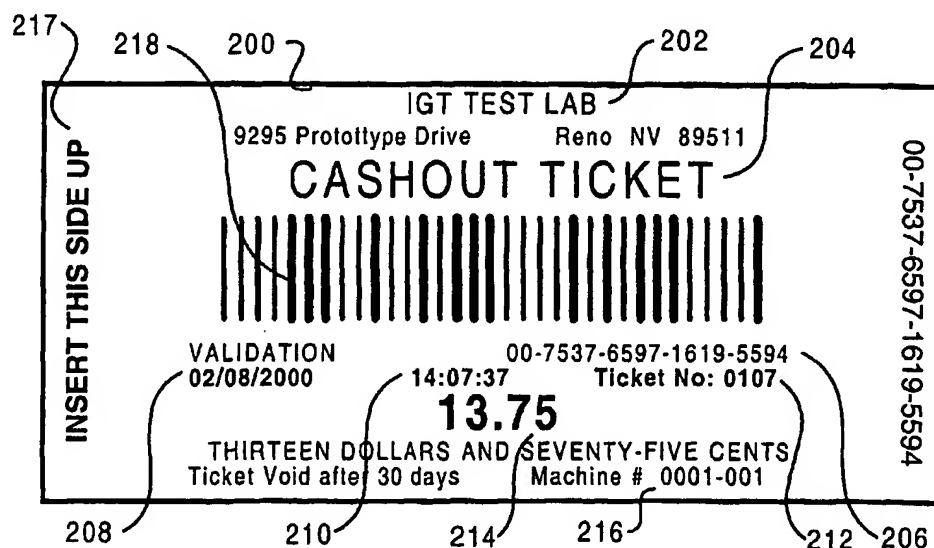
PCT

(10) International Publication Number
WO 02/022223 A3

- (51) International Patent Classification⁷: **G07F 17/32** (74) Agent: **WEAVER, Jeffrey, K.**; Beyer Weaver & Thomas, LLP, 2030 Addison Street, P.O. Box 778, 7th Floor, Berkeley, CA 94704 (US).
- (21) International Application Number: **PCT/US01/29112**
- (22) International Filing Date:
12 September 2001 (12.09.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
09/660,984 13 September 2000 (13.09.2000) US
- (71) Applicant: **INTERNATIONAL GAME TECHNOLOGY** [US/US]; 9295 Prototype Drive, P.O. Box 10580, Reno, NV 89511 (US).
- (72) Inventors: **PRASAD, Bhavani**; 9738 Thunder Mountain Way, Reno, NV 89511 (US). **ESPIN, Marc**; 5226 Canyon Run Drive, Sparks, NV 89436 (US). **ROWE, Richard, E.**; 4685 Spring Drive, Reno, NV 89502 (US).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:
— with international search report

[Continued on next page]

(54) Title: TRANSACTION SIGNATURE



(57) Abstract: The present invention provides systems and methods for protecting transaction information stored in a database of a gaming network. To accomplish this, a transaction signature is generated each time the user completes a transaction on a gaming machine. The transaction signature is generated using transaction information from a particular transaction. The transaction signature and transaction information are stored together in a network database. Upon subsequent access to the transaction information in the database, the transaction signature for the transaction information is recalculated based on the transaction information at that time. The new transaction signature is then compared to the transaction signature previously stored. Any differences between the two transaction signatures may be used to signal unauthorized alteration in the database transaction information.

WO 02/022223 A3



(88) Date of publication of the international search report:
30 January 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Inter of Application No
PCT/US 01/29112

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F17/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|------------|--|-----------------------|
| X | WO 98 47113 A (ORUS HERVE ;FOGLINO JEAN JACQUES (FR); GEMPLUS CARD INT (FR)) 22 October 1998 (1998-10-22) page 4, line 7 - line 30 page 10, line 5 -page 11, line 21 page 13, line 30 -page 14, line 6 abstract; figures --- | 1-30 |
| X | WO 98 26537 A (SCHMID ALFRED ;ASCOM SYSTEC AG (CH)) 18 June 1998 (1998-06-18) page 4, line 13 -page 5, line 3 page 10, line 19 -page 11, line 8; figures --- | 1,21-24 |
| X | WO 99 65579 A (ARISTOCRAT LEISURE IND PTY LTD ;BOND EUGENE THOMAS (US)) 23 December 1999 (1999-12-23) page 5, line 19 - line 29 page 7, line 4 - line 20; figure 2 --- | 1-13 |
| A | --- | 14-20 |
| | --- -/-- | |

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the International filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the International filing date but later than the priority date claimed

- *T* later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- *Z* document member of the same patent family

Date of the actual completion of the International search

12 June 2002

Date of mailing of the International search report

20/06/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Reule, D

INTERNATIONAL SEARCH REPORT

Inter Application No
PCT/US 01/29112

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|------------|---|-----------------------|
| A | EP 0 555 565 A (BALLY WULFF AUTOMATEN GMBH) 18 August 1993 (1993-08-18) column 5, line 39 -column 6, line 58; figures 1A-B,2,4,5 ----- | 14-20, 25-30 |
| A | US 6 012 832 A (SORENSEN DENNIS WILLARD ET AL) 11 January 2000 (2000-01-11) abstract; figures 1,2 ----- | 14-20, 25-30 |
| A | US 6 048 269 A (BURNS JAMES G ET AL) 11 April 2000 (2000-04-11) column 2, line 27 - line 47; figures 2-4 ----- | 14,25-30 |
| A | US 5 643 086 A (ALCORN ALLAN E ET AL) 1 July 1997 (1997-07-01) column 7, line 41 -column 8, line 26 ----- | 1-20 |
| A | GB 2 121 569 A (BALLY MFG CORP) 21 December 1983 (1983-12-21) page 2, line 60 -page 3, line 50 ----- | 1-20 |

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inten I Application No

PCT/US 01/29112

| Patent document cited in search report | | Publication date | Patent family member(s) | Publication date |
|---|---|---------------------|---|--|
| WO 9847113 | A | 22-10-1998 | FR 2762118 A1 AT 205004 T AU 724023 B2 AU 7050198 A BR 9806199 A CA 2258149 A1 CN 1228181 T DE 69801500 D1 DE 69801500 T2 EP 0981808 A1 ES 2163863 T3 WO 9847113 A1 JP 2001506031 T US 2002047044 A1 | 16-10-1998 15-09-2001 07-09-2000 11-11-1998 18-09-2001 22-10-1998 08-09-1999 04-10-2001 11-04-2002 01-03-2000 01-02-2002 22-10-1998 08-05-2001 25-04-2002 |
| WO 9826537 | A | 18-06-1998 | WO 9826537 A1 EP 0947072 A1 | 18-06-1998 06-10-1999 |
| WO 9965579 | A | 23-12-1999 | AU 4490699 A WO 9965579 A1 | 05-01-2000 23-12-1999 |
| EP 0555565 | A | 18-08-1993 | EP 0555565 A1 AT 166480 T DE 59209336 D1 ES 2117653 T3 | 18-08-1993 15-06-1998 25-06-1998 16-08-1998 |
| US 6012832 | A | 11-01-2000 | AU 8158198 A US 6340331 B1 WO 9859311 A1 | 04-01-1999 22-01-2002 30-12-1998 |
| US 6048269 | A | 11-04-2000 | AT 190856 T AU 6027394 A CA 2132019 A1 DE 69423555 D1 DE 69423555 T2 DE 639998 T1 EP 0639998 A1 ES 2073387 T1 GR 95300045 T1 JP 7505079 T WO 9416781 A1 US 2002034977 A1 | 15-04-2000 15-08-1994 04-08-1994 27-04-2000 09-11-2000 18-01-1996 01-03-1995 16-08-1995 31-07-1995 08-06-1995 04-08-1994 21-03-2002 |
| US 5643086 | A | 01-07-1997 | AU 6282096 A CN 1191644 A EP 0882339 A1 TR 9701723 T1 WO 9701902 A1 US 6149522 A US 6106396 A ZA 9700320 A | 30-01-1997 26-08-1998 09-12-1998 21-04-1998 16-01-1997 21-11-2000 22-08-2000 22-09-1997 |
| GB 2121569 | A | 21-12-1983 | AU 1432583 A BE 896722 A1 BR 8302453 A DE 3316414 A1 DK 211683 A ES 522284 D0 | 17-11-1983 01-09-1983 17-01-1984 22-12-1983 13-11-1983 16-05-1984 |

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter d Application No

PCT/US 01/29112

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---------------------|----------------------------|---------------------|
| GB 2121569 | A | ES 8405185 A1 | 01-09-1984 |
| | | FR 2527359 A1 | 25-11-1983 |
| | | FR 2533722 A1 | 30-03-1984 |
| | | IT 1168870 B | 20-05-1987 |
| | | NL 8301708 A | 01-12-1983 |
| | | NO 831648 A | 14-11-1983 |
| | | PT 76671 A ,B | 01-06-1983 |
| | | SE 8302671 A | 13-11-1984 |